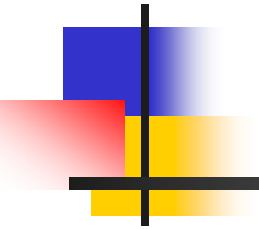


Network Security

Prof Chik How Tan
NISlab
Gjøvik University College
Chik.tan@hig.no

In this note, some of the diagrams and materials are taken from Internet

Network

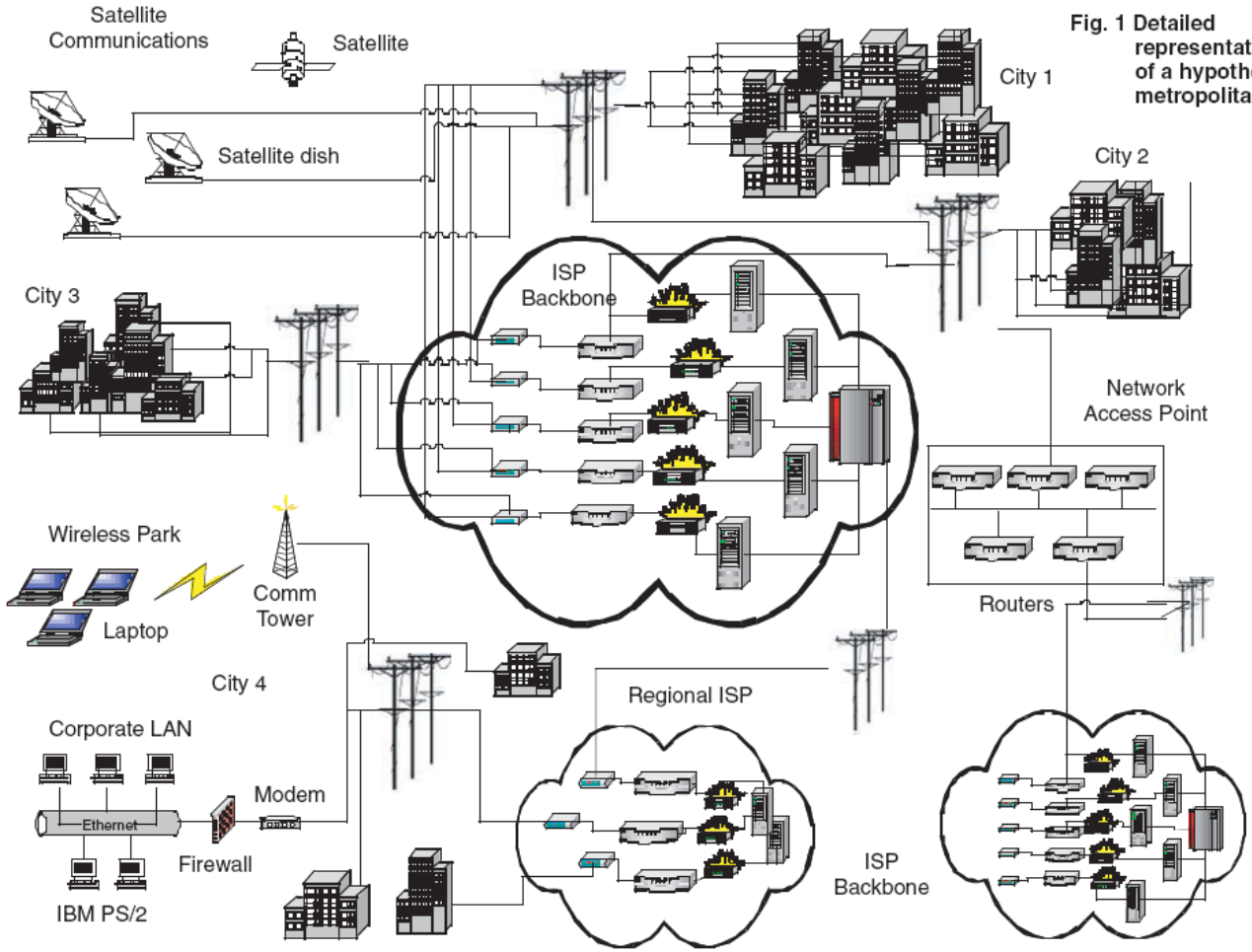
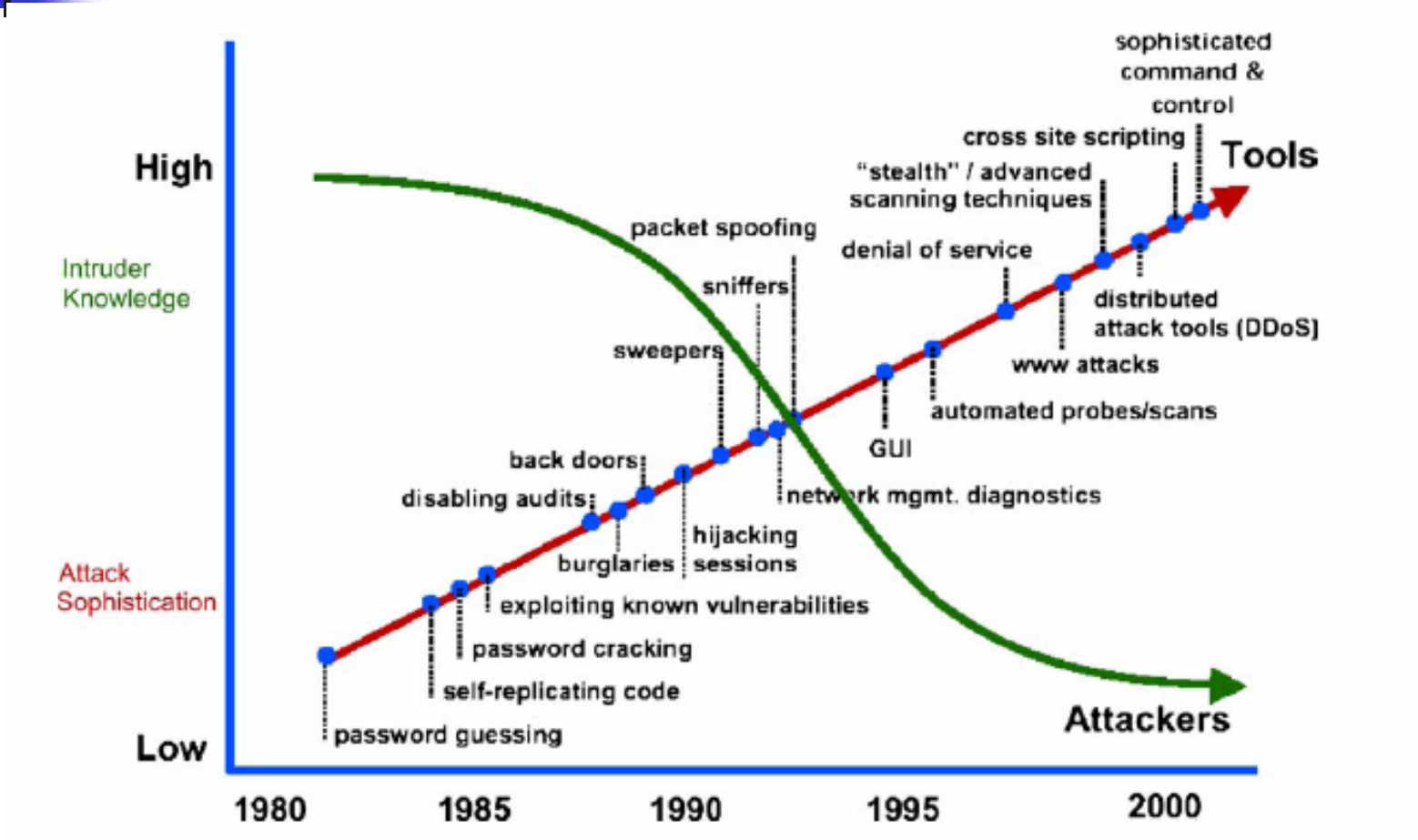
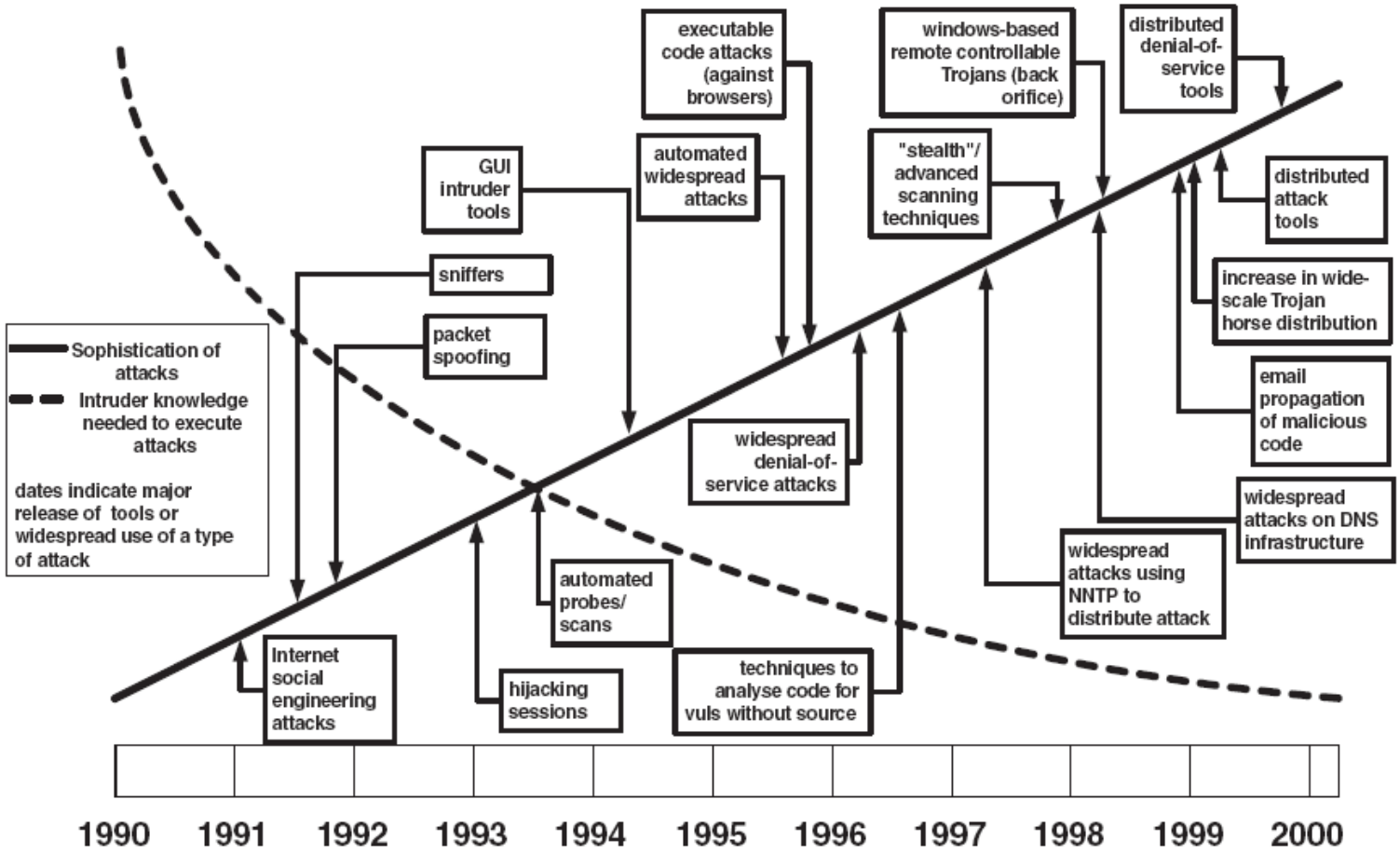


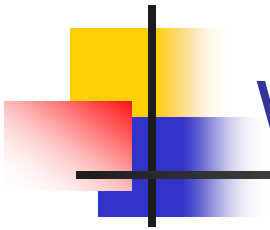
Fig. 1 Detailed representation of a hypothetical metropolitan ISP

Evolution of Attacks



Evolution of Network Attacks

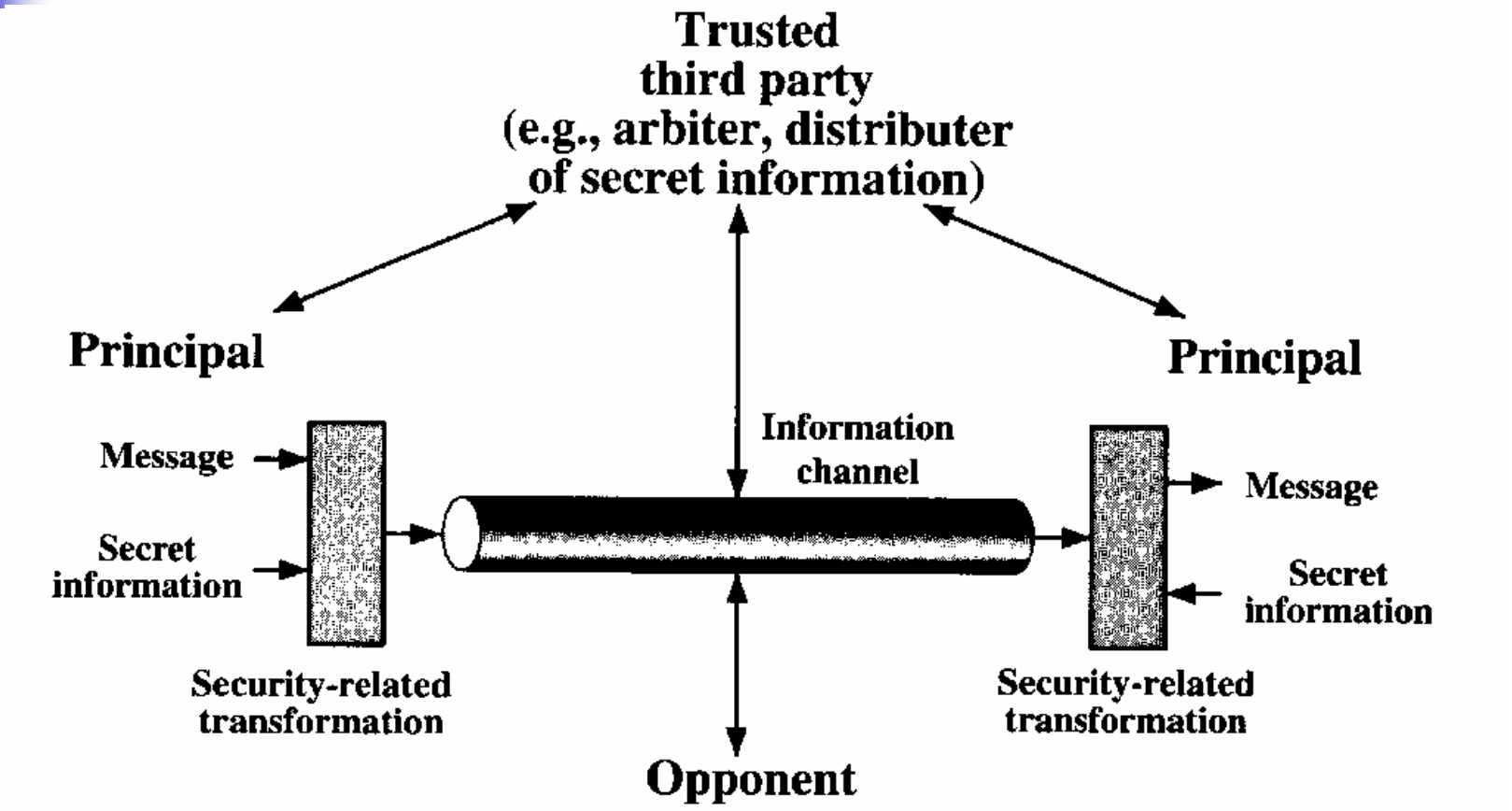


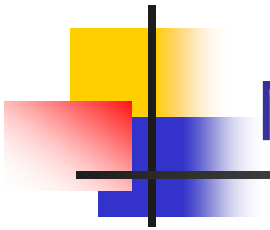


What is Network Security ?

- Network security is defined as the proper safeguarding of all components associated with a network, including data, media, and infrastructure.
- A comprehensive approach to network security involves four essential elements, namely, accurate threat assessment, use of the best cryptographic tools available, deployment of effective network access control products, and detection-protection system (includes intrustion detection system, virus scanner and audit, etc).

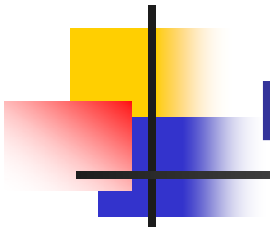
Network Security Model





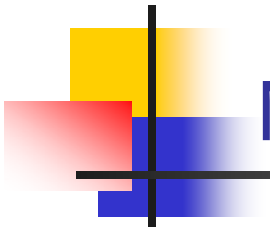
Motivation of Attacks

- Government and military : Trying to access information of national strategic importance.
- Business : obtaining information with regards to competitiveness such as design information and source code.
- Financial : Trying to gain with direct financial return. For example stealing of credit card details, or transferring money from accounts.
- Terrorist : These groups are realizing that more damage can be done through attacks on computers rather than traditional means.
- Grudge : Personal reason dictate destruction of computing resources
- Fun : Wanting to gain access more for enjoyment or enhancement of reputation than any potential profit.



Definitions

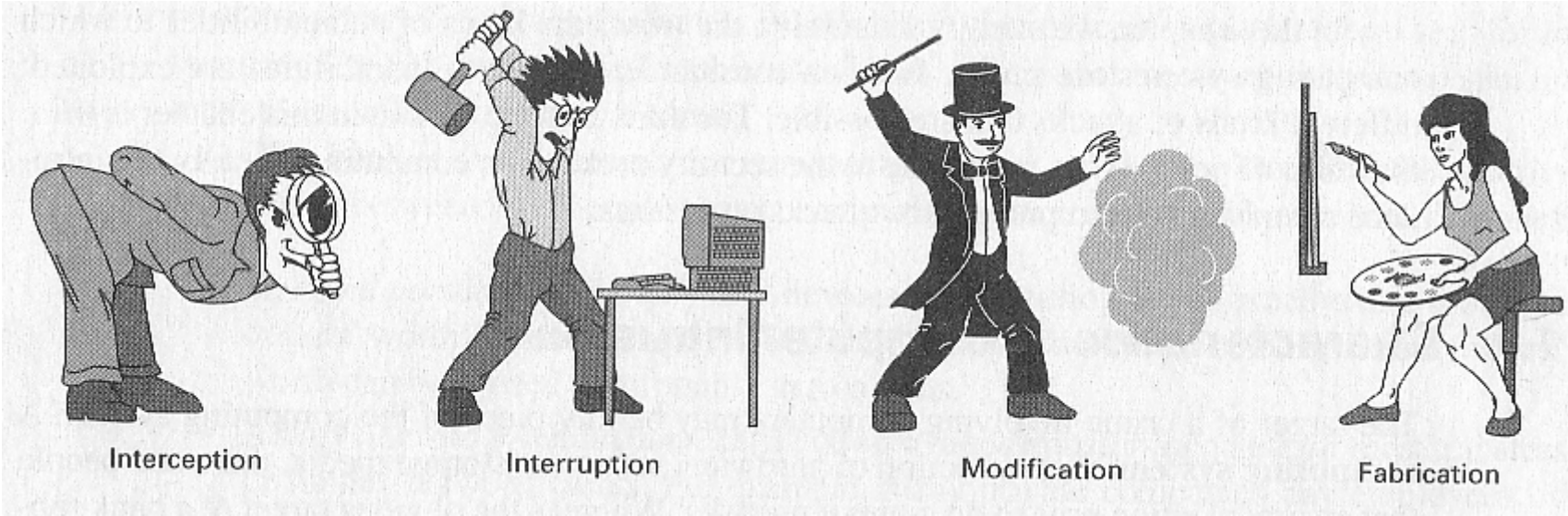
- Vulnerability is an inherent weakness in the design, configuration, implementation of a network or system. This can take any form and can be malevolent, accidental, or simply an act of nature.
- Threats is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. Human attacks are examples of the threats.
- Attack is a specific technique used to exploit a vulnerability.
- For example, a threat could be a denial of service. A vulnerability is in the design of the operating system, and and an attack could be a “ping of death”



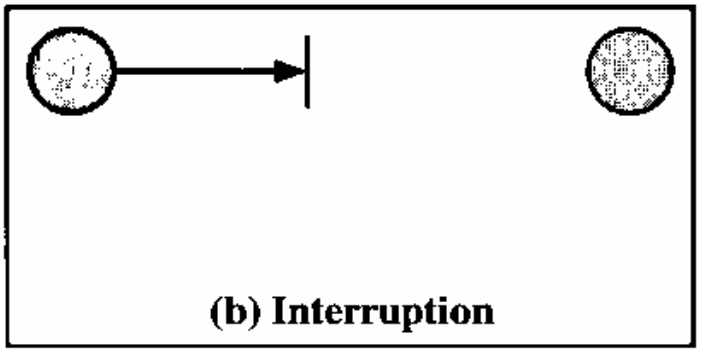
Network Security Threats

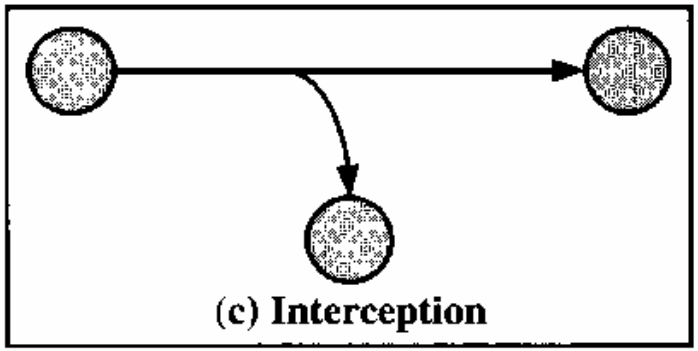
- Interception: An unauthorized party gains access to an asset (information)
- Interruption: An asset of the system is destroyed or becomes unavailable or unusable
- Modification: An unauthorized party not only gains access to but tampers with an asset
- Fabrication: An authorized party inserts counterfeit objects into the system
- Intrusion: An unauthorized party gain access to the system

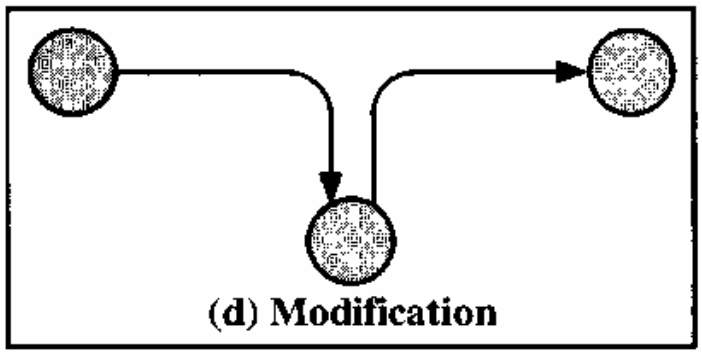
Network Security Threats (Cont'd)

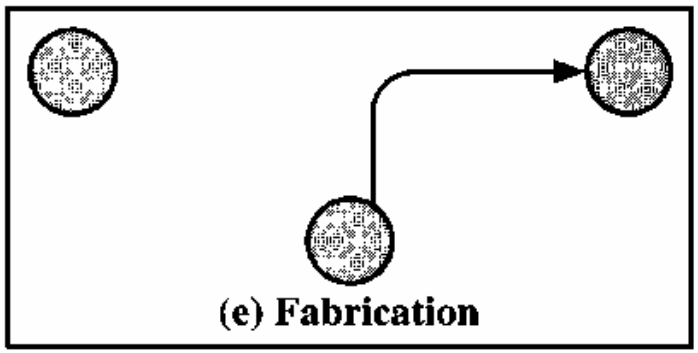


Network Security Threats (Cont'd)

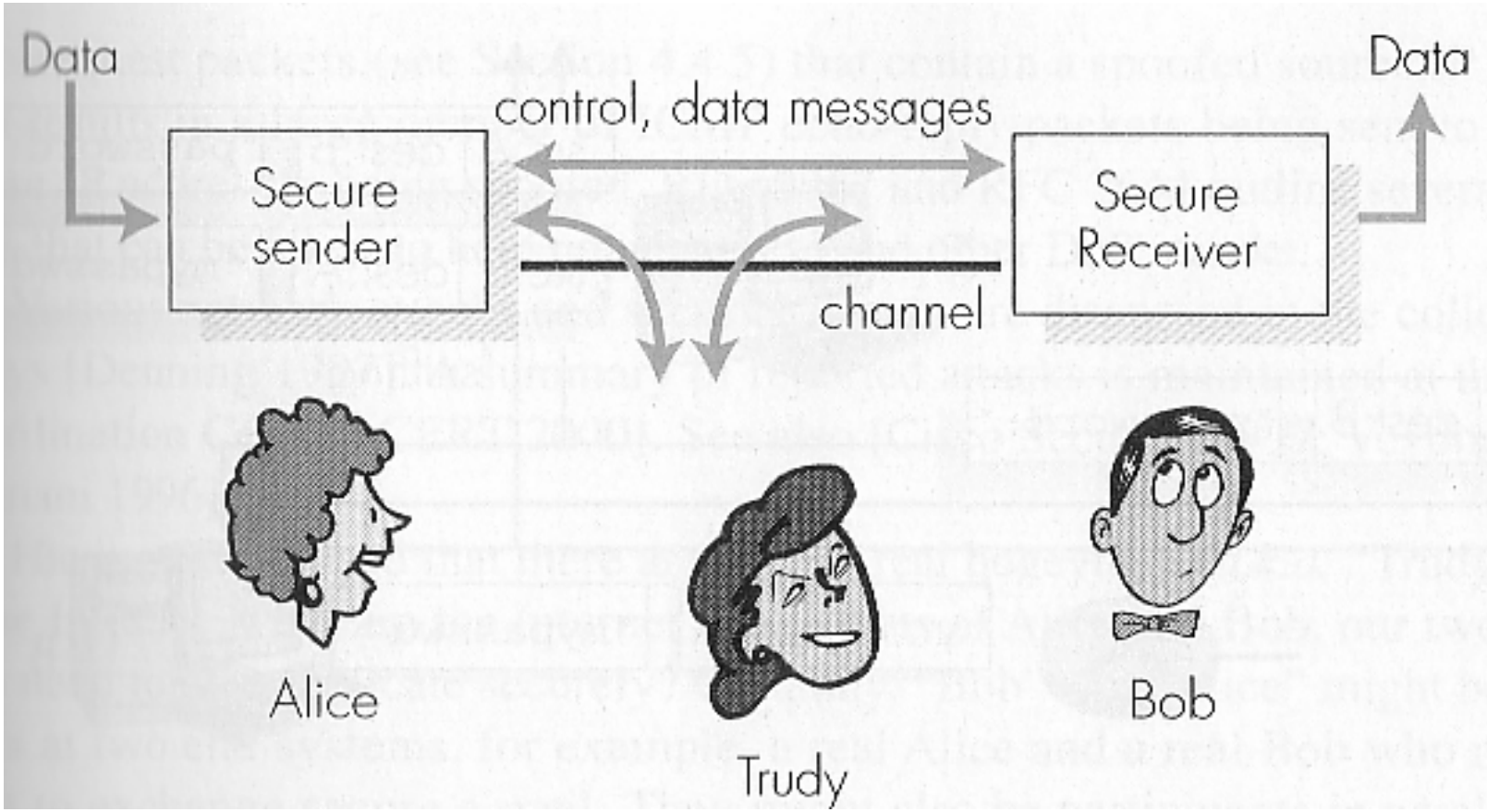


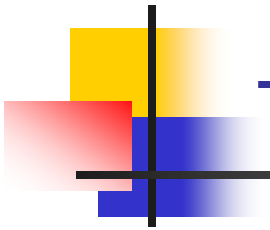






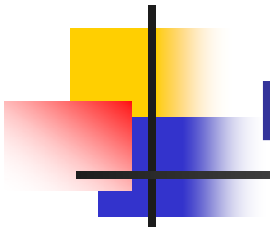
Interception





Threat Models

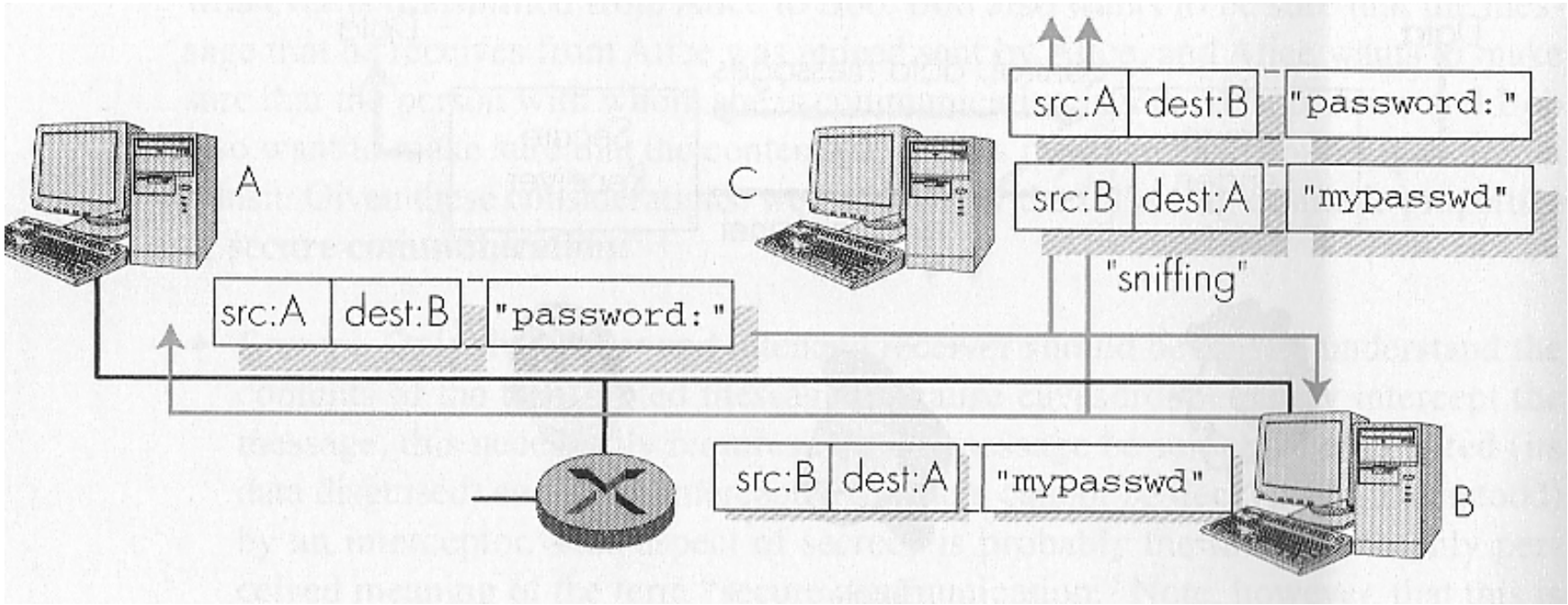
- Wiretapping attack
- Traffic Analysis
- Denial of service
- Packet sniffing
- IP spoofing
- Routing Attacks



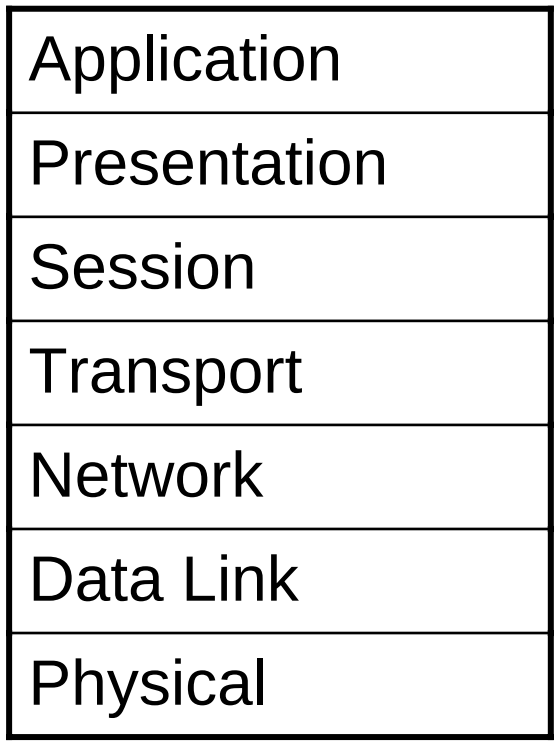
Denial Of Service

- SYN flooding : send large number of SYN packets and never acknowledge of the replies
- Smurfing : This exploits the Internet Control Message Protocol (ICMP), which enable to send an echo packet to a remote host to check whether it is alive
- Distributed DOS: an attacker subverts a large number of machines over a period of time, or on a given signal, these machines all start to bombard the target site with messages.

Packet Sniffing



Open System Interconnection (OSI) Reference model



File transfer, e-mail

ASCII Text, sound

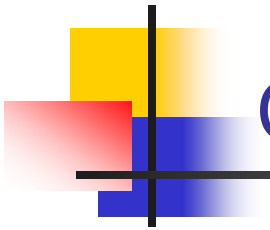
Establish/manage connection

End-to-end communication

Routing, addressing :IP

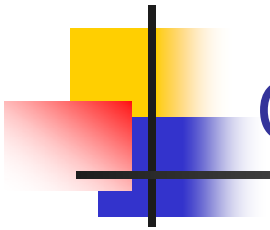
Two party communication : LAN

Transmit signals : cable



OSI Reference model (Cont'd)

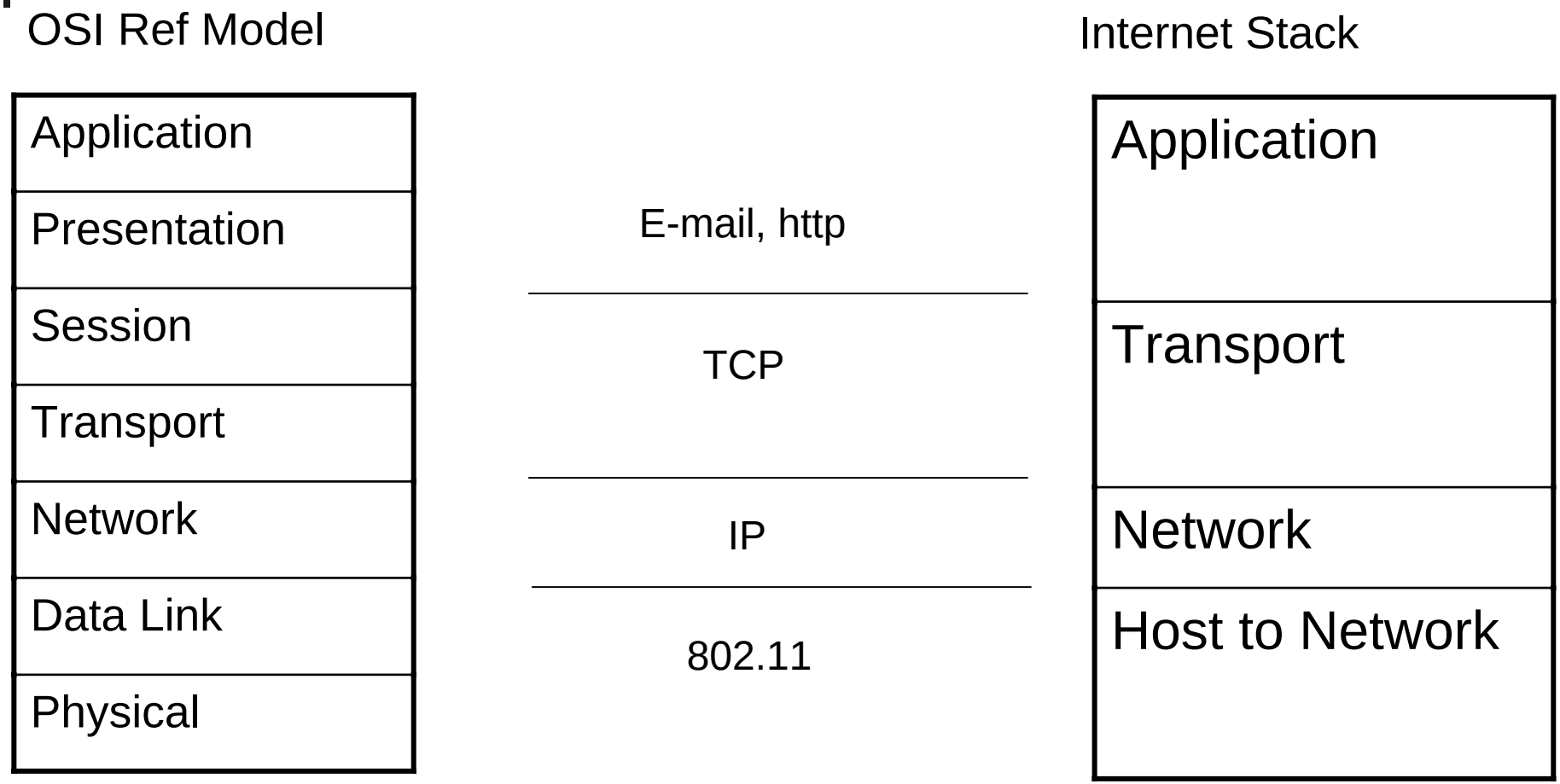
- The *physical* layer transforms the information (represented in bits) to actual signals which can be transported by physical transmission medium.
- The *link* layer provides the network layer with a reliable transfer facility. It is responsible for error detection, transmission errors, possible retransmission.
- The *network* layer establishes network wide connection, and includes facilities such as network routing.
- The *transport* layer provides the session layer with a data transfer facility that is independent of the type of network actually used

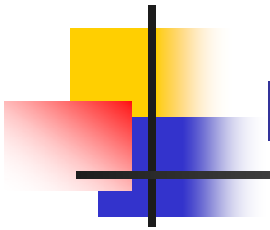


OSI Reference model (Cont'd)

- The *session* layer establishes and synchronizes the communications between applications.
- The *presentation* layer converts from an abstract syntax (eg. ASCII) and vice versa.
- The *applications* layer enables applications to get access to distributed information services. For example, an application could get access to a remote computer and download files from it.

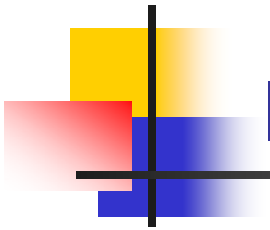
Internet Stack





Internet Stack (Cont'd)

- The *Host-to-network* layer connects the host to the network using some kind of protocol. It contains several sublayers. For example, MAC (Medium Access Control) .
- The *Network* layer is essential in the model. Its goal is to permit hosts to send packets into any network and make sure that these package travel to the correct destination. These packages may arrive in a different order than they were sent but it is up to the higher layers to re-arrange them if necessary.
- The *Transport* layer has been implemented with two different protocols: TCP and UDP

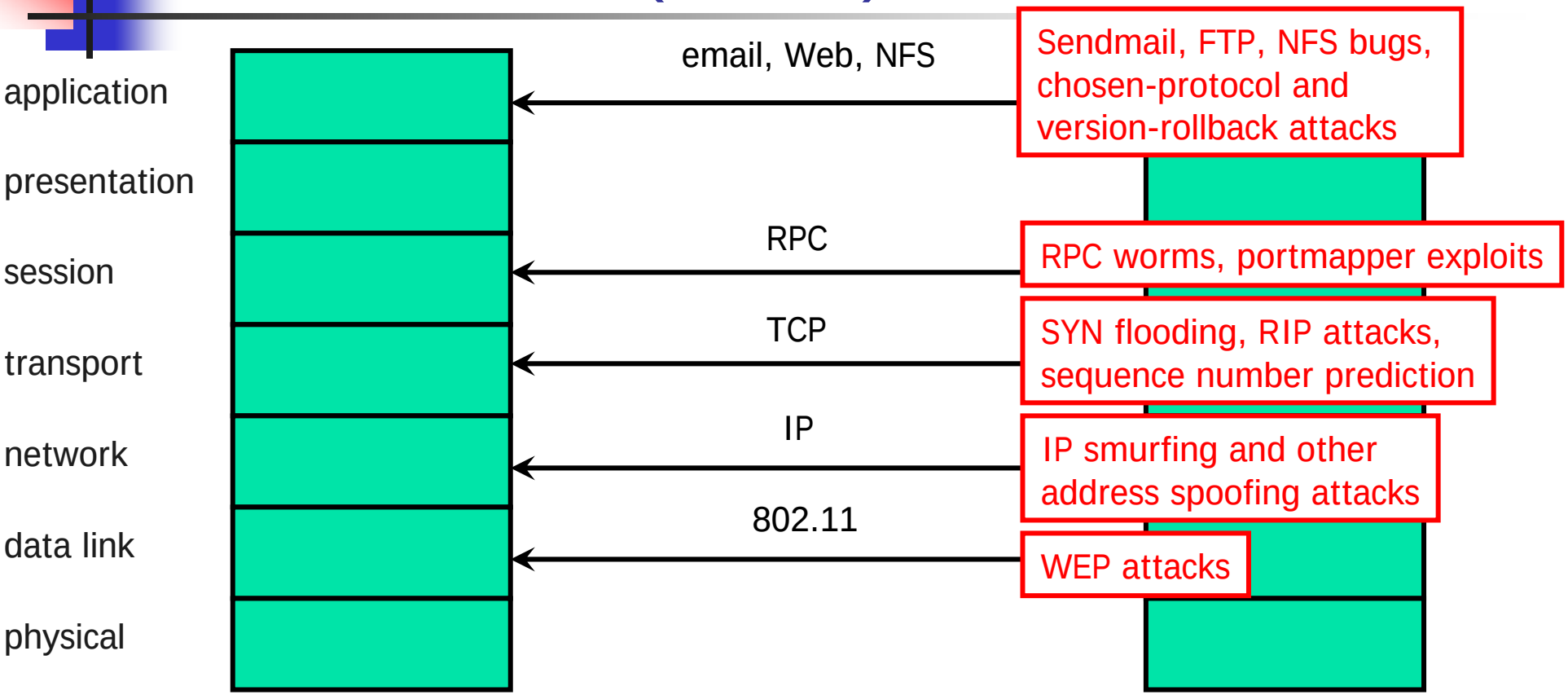


Internet Stack (Cont'd)

- TCP is a reliable connection oriented protocol. This entails that a connection is established between the source and target machine.
- UDP is an unreliable, connectionless protocol. In this case, there is no connection set-up between the originator and target machine.

- The *Applications* layer contains the regular Internet services such as HTTP, SMTP, ftp, etc.

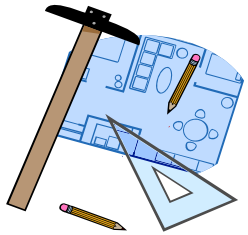
Network Stack (Cont'd)



Only as secure as the single weakest layer...

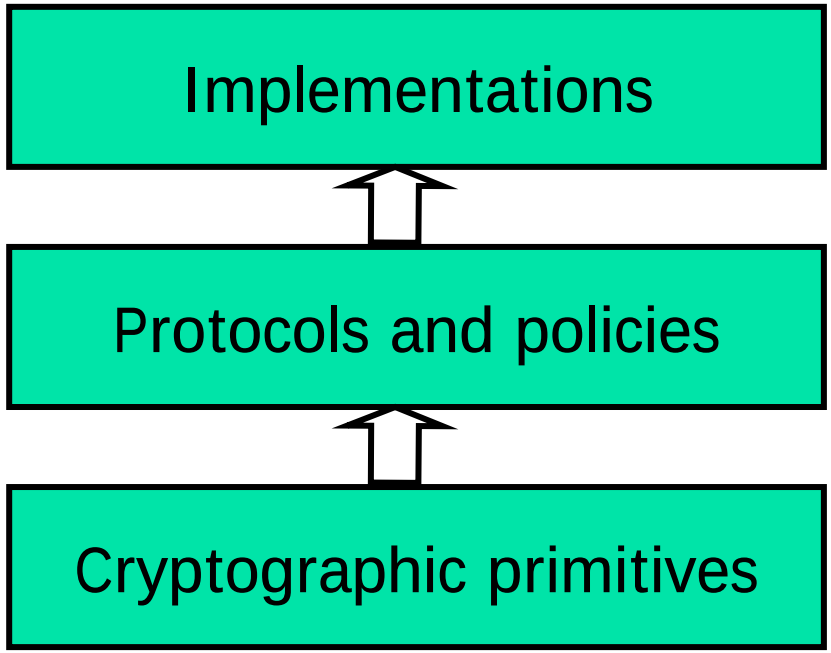
Network Defenses

Systems



Blueprints

Building blocks

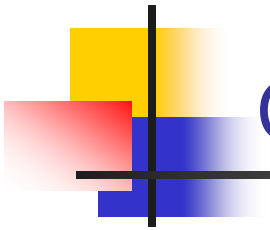


Firewalls, intrusion detection...

SSL, IPSec, access control...

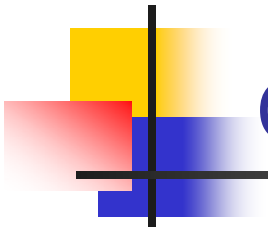
RSA, DSS, SHA-1...

...<u>all</u> defense mechanisms must work correctly and securely



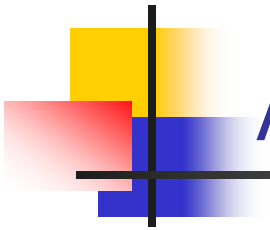
OSI Security Architecture

- 1989 : ISO/IEC 7498
- 1991 : ITU-T adopted as X.800
- Early 1990 : IRTF Privacy and Security Research Group (PSRC) adapted in Internet security architecture as an Internet draft



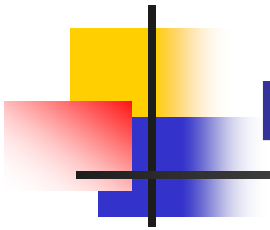
OSI Security Services

- Authentication services
- Access control services
- Data confidentiality
- Data integrity
- Non-repudiation services



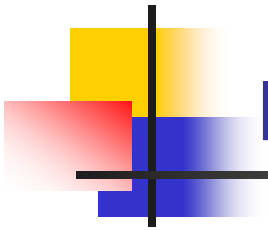
Authentication Services

- To provide for authentication of communicating peer entities or for the authentication of data origin
- A peer entity authentication
  - To verify that a peer entity in an association is the one claim to be
- A data origin authentication
  - The sources of data received to be verified to be as claimed



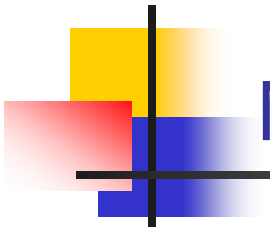
Data Confidentiality

- Information is not made available or disclosed to unauthorized individuals, entities, or processes
- Connection confidentiality
  - To provide confidentiality of all data transmitted in a connection
- Connectionless confidentiality
  - To provide confidentiality of all data transmitted in a connectionless
- Traffic flow confidentiality
  - To provide protection of information that may otherwise be compromised or indirectly derived from a traffic analysis



Data Integrity

- Information is not altered or destroyed in an unauthorized way
- To ensure that the information is not changed

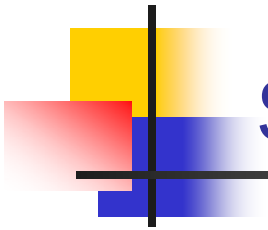


Non-repudiation

- To prevent that one of the entities involved in a communication later denies having participated in all or part of the communication.
- A non-repudiation service with proof of origin
  - To provide the recipient of a message with a proof of origin
- A non-repudiation service with proof of delivery
  - To provide the sender of a message with a proof of delivery

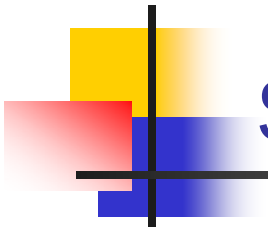
Cryptographic Services

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the Net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques



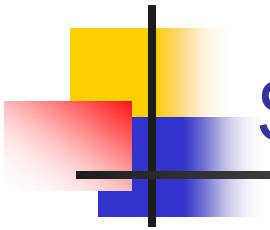
Security Mechanisms

- Encipherment
- Digital signature mechanisms
- Access control mechanisms
- Data integrity mechanisms
- Authentication exchange mechanisms
- Traffic padding mechanisms
- Routing control mechanisms
- Notarization mechanisms



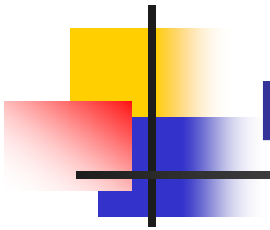
Security Management

- System security management
- Security service management
- Security mechanism management
- For Example,
  - Network management station is a system that supports a network management protocol and the applications necessary for it to process and access information from managed entities on the network -- SNMP



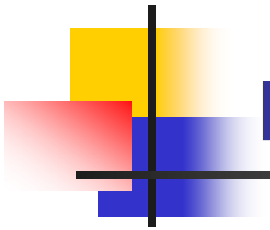
Security Policy

- Managing risk:
- Ensuring business continuity
- Defining responsibilities, expectations and acceptable behaviors
- Discharging fiduciary duty and complying with any regulatory requirements
- Protecting the organization from liability
- Ensuring information integrity and confidentiality



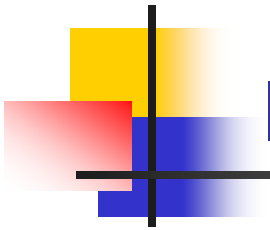
Developing Security Policy

- Identifying the organization's assets;
- Defining the risks;
- Defining how information assets are to be managed;
- Defining how information assets are to be accessed and what process will be used for authentication;
- Defining clearly and in detail what does and does not constitute appropriate use of company owned electronic media and services;
- Clearly defining what kind of information may be accessed and distributed and by what means;



Developing Security Policy (Cont'd)

- Defining what controls are to be put in place;
- Notifying users of monitoring and auditing procedures, information disclosure, and consequences for noncompliance;
- Identifying those responsible for security enforcement and how policies and procedures will be enforced;
- Developing steps to be taken in the event of noncompliance with policy, a security breach, or a disaster.

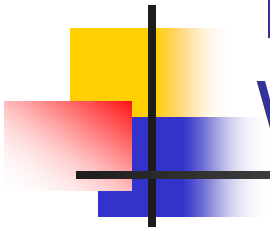


Implementing Security Policy

- Developing a written security policies and procedures manual;
- Developing an end user awareness and education program;
- Developing a process for policy enforcement and procedure implementation;
- Developing a process for the periodic review and updating of policies and procedures.

Internet Engineering Task Force Security Working Group

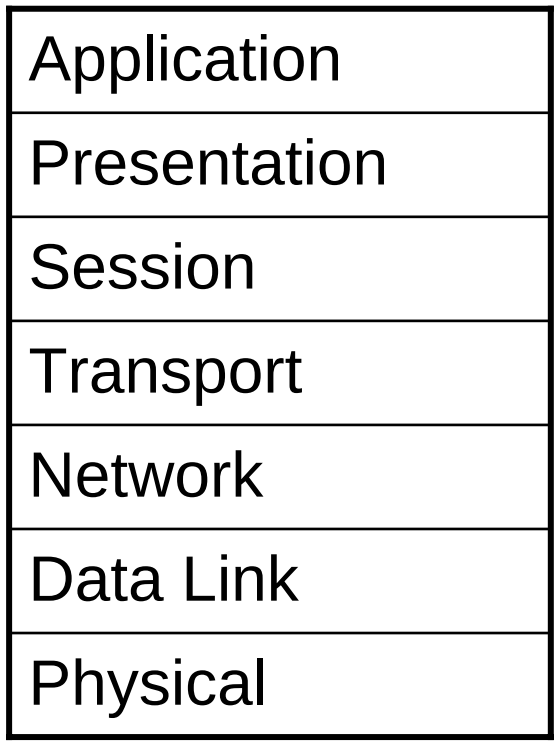
- Authentication Firewall Traversal (AFT)
- Common Authentication Technology (CAT)
- Domain Name Security (DNSSEC)
- IP Security Protocol (IPSEC)
- An Open Specification for Pretty Good Privacy (OPENPGP)
- One Time Password Authentication (OTP)
- Public Key Infrastructure based on X.509 (PKIX)
- Secure Shell (SECSH)
- S/MIME Mail Security (SMIME)



Internet Engineering Task Force Security Working Group

- Simple Public Key Infrastructure (SPKI)
- Transport Layer Security (TLS)
- Web Transaction Security (WTS)

Security Solutions in (OSI) Reference model



S/MIME, Secured FTP, PGP

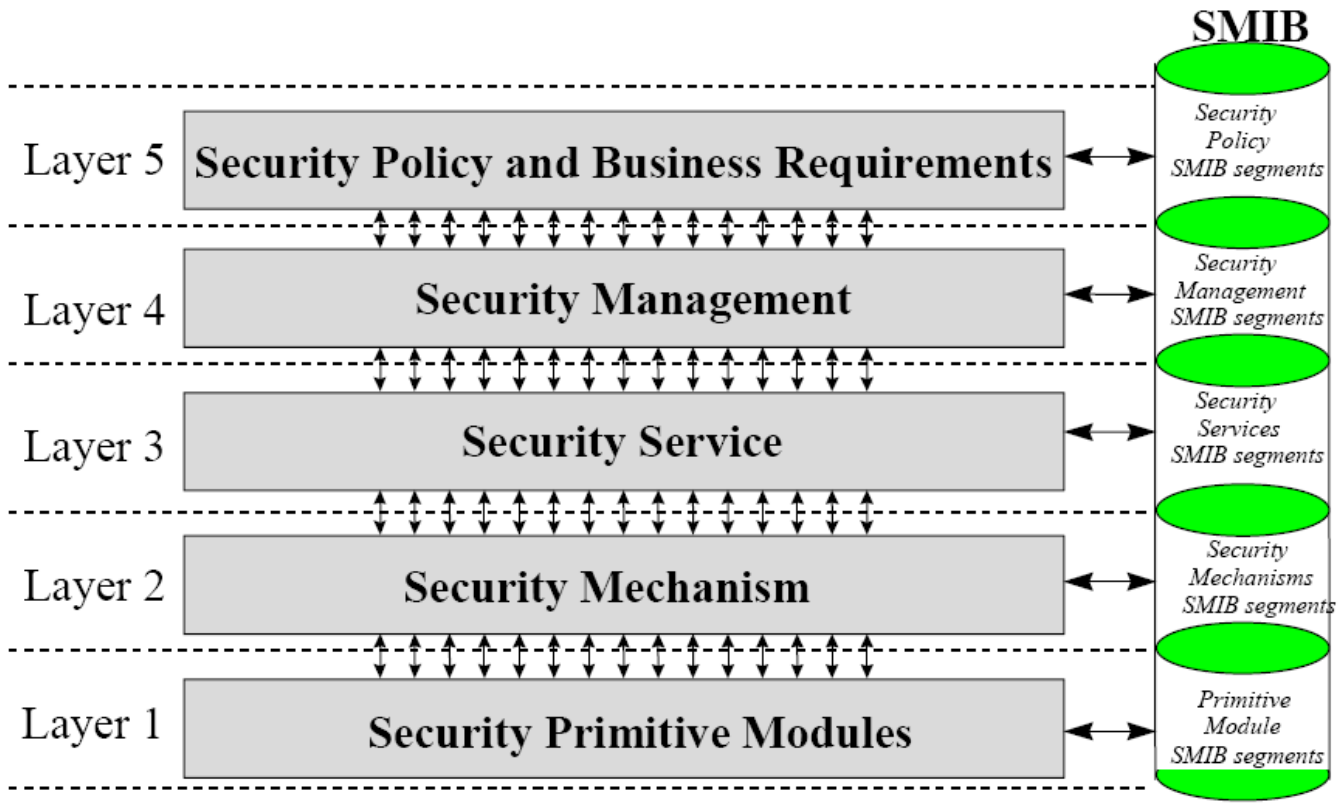
SSH, SSL, TLS

IPSEC, VPN

Link encryption

Optical Transmission

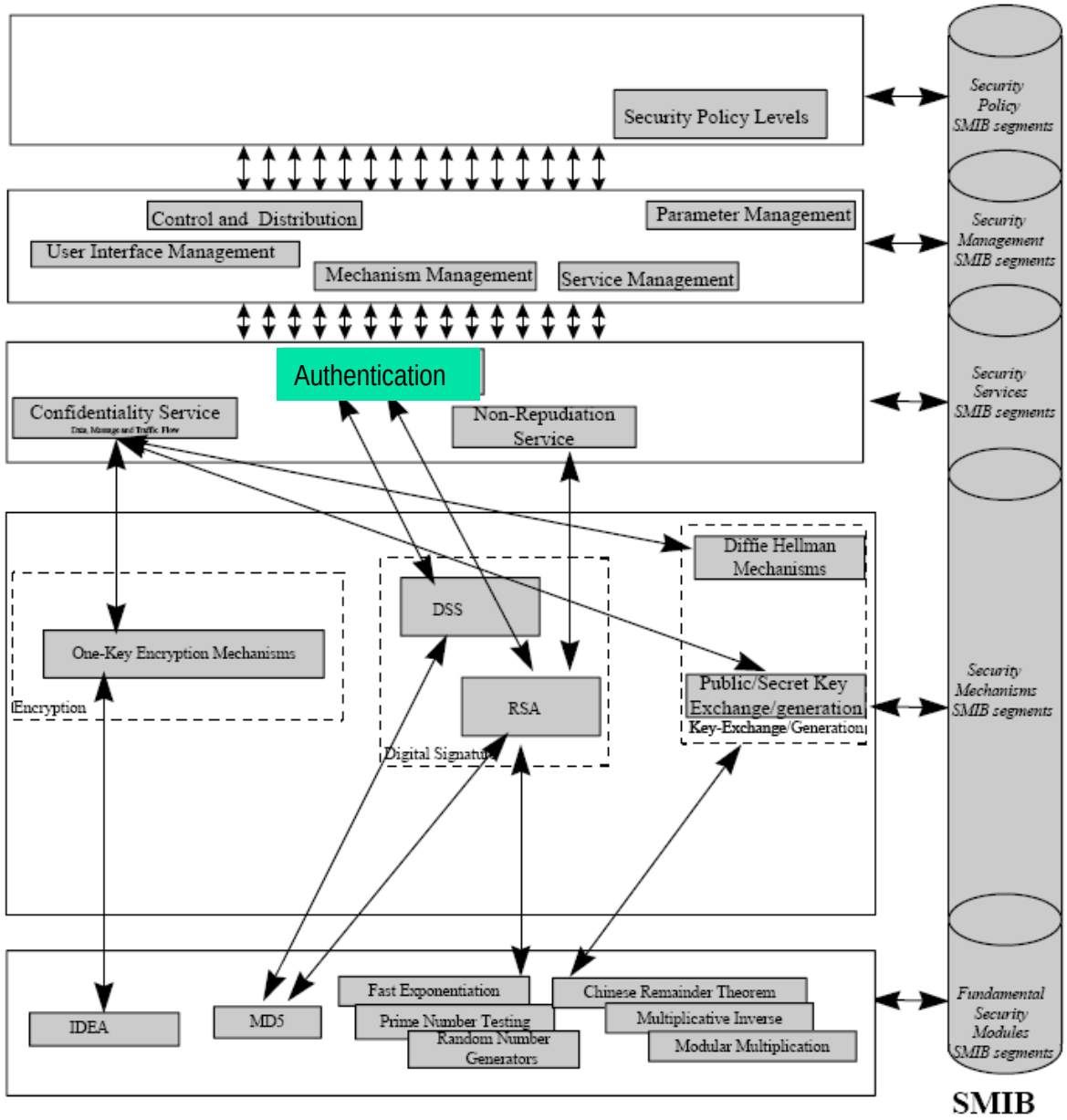
Security Management System



SMIB : Security Management Information Base

Security Management System (Cont'd)

- Layer 5 – Security Policy and business requirements
  - prevent and detect security violations, disaster recovery, personnel risk analysis, legal views and actions
- Layer 4 – Security Managements
  - Control and distribution, event logging, monitoring, parameter management, user interface, service management, mechanism management, recovery
- Layer 3 – Security Services
  - Confidentiality, integrity, authentication, access control, non-repudiation, availability
- Layer 2 – Security Mechanisms
  - DSS, RSA, mode of operations, cryptographic protocols, etc.
- Layer 1 – Security Primitive Modules
  - DES, AES, SHA-1/2, large number arithmatic, random number sequence, elliptic curve, etc


Security Policy Levels
Control and Distribution
Parameter Management
User Interface Management
Mechanism Management
Service Management
Authentication
Confidentiality Service
Non-Repudiation Service
Diffie Hellman Mechanisms
DSS
One-Key Encryption Mechanisms
Encryption
RSA
Public/Secret Key Exchange/generation
Key-Exchange/Generation
Digital Signature
IDEA
MD5
Fast Exponentiation
Prime Number Testing
Random Number Generators
Chinese Remainder Theorem
Multiplicative Inverse
Modular Multiplication
Security Policy SMIB segments
Security Management SMIB segments
Security Services SMIB segments
Security Mechanisms SMIB segments
Fundamental Security Modules SMIB segments
SMIB